Mida saavad tööandjad teha, et kaitsta oma ettevõtteid küberrünnakute eest?

Riigi Infosüsteemi Ameti poolt eelmise aasta septembris avaldatud andmete kohaselt kaotavad Eesti ettevõtted küberkurjategijatele aastas üle miljoni euro. See number on siiski vaid jäämäe tipp, sest hõlmab vaid ametile edastatud andmeid. Küberkuritegude kurba statistikat arvesse võttes on selge, et küberhügieeni järgimist töötajate poolt tuleks pidada sama oluliseks kui kohustust käsi pesta.

Küberturvalisuse riskide leevendamiseks on soovitatav rakendada mitmekihilist lähenemisviisi, sest küberohtude vastane kaitse hõlmab üldjoontes kolme komponenti: inimesed (siin peetakse silmas töötajate teadlikkust küberohtudest ja küberturvalisuse parimate tavade järgimist), protsessid (organisatsioonis kehtestatud protseduurid küberohtude ennetamiseks, avastamiseks ja neile reageerimiseks) ja tehnoloogia (küberohtude leevendamiseks mõeldud tehnoloogiliste vahendite rakendamine, näiteks tulemüürid, pahavaratõrje tarkvara, mitmeastmeline autentimine jne). Isegi kui organisatsioonis on kehtestatud nõuetekohased protseduurid ja kasutatakse kaasaegseid küberturvalisuse tehnoloogiaid, võivad töötajad siiski endast märkimisväärset turvariski kujutada. Näiteks kui töötajad ei ole küberturvalisuse parimatest tavadest teadlikud või ei järgi neid, võivad nad kergesti langeda andmete õngitsemise ohvriks. Kui see õnnestub, saavad küberkurjategijad juurdepääsu ettevõtete konfidentsiaalsetele andmetele ja varadele.

Euroopa Liidu õigusaktidega (Euroopa Liidu andmekaitse üldmäärus) kehtestati kohustus kaitsta vastutava töötleja poolt töödeldavaid isikuandmeid ning rakendada sellega seoses asjakohaseid tehnilisi ja korralduslikke meetmeid. Selleks peavad organisatsioonid kaitsma oma töötajate ja klientide andmeid, mida kasutatakse mistahes sisemistes protsessides, süsteemides, teenustes või toodetes. Kuid peale isikuandmete kaitse ei kohusta seadused siiski neid eraettevõtteid, kes ei osuta hädavajalikke ega digitaalteenuseid, konkreetseid küberturvalisuse reegleid järgima. Seega on iga äriühingu ülesanne hinnata oma konkreetse äritegevusega seotud riske ja rakendada meetmeid nende vähendamiseks. Võttes arvesse, et täna hoitakse ja hallatakse andmeid ärisaladuste, intellektuaalomandi ja muu väärtusliku äriteabe kohta digitaalsel kujul, võib see info olla küberrünnakutele avatud. Kahjuks on praktikas turvaoskuste puudumine või töötajate hooletus üks peamisi andmelekkeid põhjustavaid tegureid.

Küberturvalisuse reeglid

Küberturvalisuse reeglite järgimist saab muuta töötajatele kohustuslikuks, kui need on õigesti dokumenteeritud. Küberturvalisuse reeglite järgimise kohustuse võib kehtestada töölepingus või ametijuhendis. Kui küberturvalisuse reeglid koostatakse töölepingust eraldi (töölepingu lisana või ametijuhendina), siis selleks, et need oleksid töötajatele siduvad, tuleb neid töötajatele tutvustada ja mõlema poole poolt allkirjastada. Tuleb arvestada, et kui reeglid on allkirjastatud, võib tööandja neid muuta ainult *töötaja* nõusolekul (sarnaselt töölepingu muude tingimuste muudatustele).

Küberturvalisuse reeglid sätestavad tavaliselt andmetega turvalise töötamise ja turvariskide vähendamise juhised, sealhulgas interneti kasutamise, isiklike ja ettevõtte seadmete kaitse, e-posti side turvalisuse, paroolihalduse, kaugtööga seotud konkreetsete riskide maandamise jms juhised. Küberturvalisuse reeglid sisaldavad ka töötajatele mõeldud suuniseid selle kohta, kuidas erinevaid küberohte ära tunda ja turvarikkumiste korral tegutseda.

Küberturvalisuse reeglites tuleks arvesse võtta töökohustuste laadiga seotud konkreetset positsiooni ja riskitaset. Standardse dokumendi kasutamine iga töötaja puhul ei ole hea mõte, sest tööandja andmetele ja tööeesmärkidele juurdepääsuõigused sõltuvad tavaliselt ametikohast. Näiteks on mõistlik koostada küberturvalisuse reeglid kontoritöötajale ja IT-spetsialistile, võttes arvesse nende ametikohtadega seotud vastutuse ja riskide erinevat taset. Mida laiem on töötaja õigus tööandja andmetele juurde pääseda ja nendega töötada, seda suuremat kahju võib tööandja potentsiaalselt kannatada, kui töötaja satub küberkuriteo ohvriks.

Küberturvalisuse reeglites kirjeldatud kohustused peaksid olema mõlema poole jaoks mõistlikud ja selged. Tööandja ei saa tugineda kohustuse rikkumisele, kui kohustused on sõnastatud ebamääraselt või heita töötajale ette spetsiifilist oskust nõudvate kohustuse mittetäitmist, mille osas tööandja ei ole vastavat koolitust pakkunud. Ebamõistlikud tingimused on ka tööandjatele kahjulikud, kuna neid ei pruugi olla võimalik kohtus maksma panna.

Töötajate koolitused

Ainuüksi küberturvalisuse reeglitest ei piisa ettevõtte kaitsmiseks küberriskide eest. Töötajate teadlikkus küberohtudest ja nende roll ettevõtte küberturvalisuse tagamisel on kahju vältimise võtmetegur. Seetõttu peab tööandja pakkuma töötajatele regulaarset turvakoolitust. Kuna andmeturbe tagamine on otseselt tööandja huvides, peab tööandja vastavalt töölepingu seadusele pakkuma selle valdkonnaga seotud töötajatele koolitust omal kulul ja maksma koolituse ajal keskmist palka.

JELIZAVETA HENNO
VANDEADVOKAAT

(+372) 66 76 440
JELIZAVETA.HENNO@NJORDLAW.EE